



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/530,122

02/23/2010

Tatsuo Nomura

63227(72039)

2625

21874 7590 11/22/2010
EDWARDS ANGELL PALMER & DODGE LLP
P.O. BOX 55874
BOSTON, MA 02205

EXAMINER

RAHMAN, MAHFUZUR

ART UNIT

PAPER NUMBER

2438

MAIL DATE

DELIVERY MODE

11/22/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/530,122	Applicant(s) NOMURA ET AL.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period **will** apply and **will** expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply **will**, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 September 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 April 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Applicant's amendment filed 09/24/2010 is acknowledged. Claims 1-6 have been amended. Claims 1-6 are examined and pending.

Response to Arguments

1. Regarding claims 1-6 rejected under 35 USC 103(a), applicant argued,
“However, there is no teaching or suggestion in Verma of image data processing means that have "different security levels," as claimed.”

The Examiner respectfully disagrees. The reference of Verma teaches access control to the data processing means based on different permission levels, which implies that data processing means must have different security levels otherwise these permission levels will be of no use in the processing of inputted image data (Paragraph 0089: in response to a print command, additionally, the thin client 224 suitably communicates with a remote DMM 232 of a second appliance 234; 0277: when data is present in the queue 7906, retrieves the data from the queue 7906, interrogates the data for destination information (job information) and passes it in a distribution process 7908 to the appropriate destination).

Further, Verma teaches that data processing means enforce different access rights which further affirms that access rights must have different levels of security that corresponds to the data processing means to process inputted image data (Paragraph 0209: the appliance 200 enforces the following un-modifiable access rights: only the

Art Unit: 2438

Administrator and the owner of a private container have full access to the respective container; Paragraph 0207: The Power User and general user can have a different appliance username and password from their domain username and password for security reasons. The appliance 200 provides a series of dedicated utilities that will allow the Administrator to define and manage the user accounts. The appliance architecture recognizes the following user archetypes: Administrator, Power User, and User).

Furthermore, Olsen discloses that data processing means are classified based on the functionalities performed by corresponding means (Paragraph 0209: Printer classification tag used to categorize printers in different groups; Paragraph 0219: Creation and assignment of categories are performed centrally using the AdmGui The billing system will use the users network login as user authentication scheme) wherein different levels of security corresponding to the processing interface enables the client to send access request to the data processing means having appropriate level of security (Paragraph 0363: Each interface is described by command, followed by arguments, and the replies to the command. Finally the security level for the command. The security level is divided into three levels. Lowest is User, second is PowerUser and above all is the Administrator. When a security level is denoted it means that level and above).

Therefore, in view of above teachings, the reference of Verma alone or at least when combined with the reference of Olsen disclose the limitations as claimed and is obvious to one of ordinary skill in the art at the time the invention was made.

Applicants amendment of claims 1, 3, 5, and 6 filed September 24, 2010 necessitated a new ground of rejection presented in this Office action. The previously presented rejections with respect to these claims have changed because new components: “at least first and second image data processing means which have different security levels ...”, “in addition to the first image data is processing means” have been added to the respective claims. Thus applicant’s arguments have been rendered moot in view of the new ground(s) of rejection.

The reference of Lunt has been introduced to address the newly added limitations. The reasons of obviousness are included below in this office action.

Claims 1-6 are now rejected under 35 U.S.C. 103(a) as being unpatentable over Verma et al. (US 2003/0115326 A1, hereinafter, Verma) in view of Lunt et al. (Patent No. US 7,110,541 B1, hereinafter, Lunt).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

Art Unit: 2438

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Verma et al. (Prior art of record, US 2003/0115326 A1, hereinafter, Verma) in view of Lunt et al. (Patent No. US 7,110,541 B1, hereinafter, Lunt).

Regarding Claim 1, Verma discloses an image processing device, comprising:
a plurality of image data processing means at least first and second image data processing means which have different security levels and which process inputted image data (Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Fig. 1: plurality of image

Art Unit: 2438

data processing means); and

one or more image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager),

wherein the image data processing requesting means have a function [to verify security levels] of the second image data processing means to which the image data processing is to be requested (Paragraph 0101: check the status of the appliance queue associated with the selected device; Paragraph 0114: the destination type is for printing the job (i.e., in response to a "print" function), the Distribution Print Agent 600 communicates with the Configuration Manager 500 to determine other details, such as queue name, and printer hostname/IP) and

then request the second image data processing means to perform distributed processing of image data in addition to the first image data processing means that is first requested to process the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202; Paragraph 0089: in response to a print command, additionally, the thin client 224 suitably communicates with a remote DMM 232 of a second appliance 234).

Verma does not explicitly disclose but Lunt from the same or similar fields of endeavor teaches verifying security levels in image processing system (Col. 4 lines 30-38: Once the policy 113 determines the security requirements, the print management system 112 identifies the specific combination of protection techniques needed to meet these requirements. The print management system 112 then routes the print job to one of the trusted printers 131 135 that can apply the appropriate protections and sets the parameters in the selected printer to apply the appropriate protection techniques to the document 140).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels as taught by Lunt in the teachings of Verma for the advantage of printing a document requiring forgery protection using a number of trusted printers (Col. 1 lines 55-57).

Regarding Claim 2, the combination of Verma and Lunt discloses the image processing device according to claim 1, wherein the image data processing requesting means have a function to select, from among the plurality of image data processing means, all other image data processing means whose security level is equal to or higher than the security level of the first image data processing means that is first requested to process the image data (Verma, Paragraph 0207: The appliance architecture recognizes the following user archetypes: Administrator, Power User, and User. The appliance 200 allows for the grouping of users into user groups. A Power User and Administrator can only create/delete a group and add/delete members to the

group. Grouping is only available for the DMM component, and is basically done to simplify the sharing of resources (Folders, etc.), and

a function to request the selected second image data processing means to perform distributed processing of the image data (Verma, Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Paragraph 0093: if the user intends to send the job to multiple destinations, then the user selects the destination printer(s) and load a previously-stored job delivery profile).

Regarding Claim 3, Verma discloses an image processing device, comprising: a plurality of image data processing means including at least first and second image data processing means which have different security levels and which process inputted image data (Paragraph 0081: The system 100 includes a network-based document service appliance 102 (i.e. iSP appliance for image Service Platform appliance) that is a document distribution solution with document management capabilities and device management support; Fig. 1: plurality of image data processing means); and

an image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager),

wherein the image data processing requesting means have a function [to verify a security level] of the second image data processing means to which the image data processing is to be requested (Paragraph 0114: the destination type is for printing the job (i.e., in response to a "print" function), the Distribution Print Agent 600 communicates with the Configuration Manager 500 to determine other details, such as queue name, and printer hostname/IP; Paragraph 0101: check the status of the appliance queue associated with the selected device) and

then request the second image data processing means to perform alternate processing of the image data (Paragraph 0201: a facility is provided to the user through which aged files (documents that were not accessed within a specified period of time) are automatically moved to an alternative location)

in place of the first image data processing means that is first requested to process the image data if the first image data processing means can no longer continue processing subsequent part of the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202).

Verma does not explicitly disclose but Lunt from the same or similar fields of endeavor teaches verifying security levels in image processing system (Col. 4 lines 30-38: Once the policy 113 determines the security requirements, the print management

Art Unit: 2438

system 112 identifies the specific combination of protection techniques needed to meet these requirements. The print management system 112 then routes the print job to one of the trusted printers 131 135 that can apply the appropriate protections and sets the parameters in the selected printer to apply the appropriate protection techniques to the document 140).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels as taught by Lunt in the teachings of Verma so the parameters of the selected trusted printer are set by a print management system to print images, including the copy evidence and/or tracing information, appropriate to the required level of protection (Col. 2 lines 21-27).

Regarding Claim 4, the combination of Verma and Lunt discloses the image processing device according to claim 3, wherein the image data processing requesting means have a function to select, from among the plurality of image data processing means, all other image data processing means whose security level is equal to or higher than the security level of the first image data processing means that is first requested to process the image data (Verma, Paragraph 0207: The appliance architecture recognizes the following user archetypes: Administrator, Power User, and User. The appliance 200 allows for the grouping of users into user groups. A Power User and Administrator can only create/delete a group and add/delete members to the group. Grouping is only available for the DMM component, and is basically done to simplify the sharing of resources (Folders, etc.), and

a function to request the selected second image data processing means to perform alternate processing of subsequent part of the image data (Verma, Paragraph 0265: subsequent "Print File" operations; Paragraph 0093: if the user intends to send the job to multiple destinations, then the user selects the destination printer(s) and load a previously-stored job delivery profile).

Regarding Claim 5, Verma discloses an image processing system, comprising: a plurality of image data processing means including at least first and second image data processing means which have different security levels and which process inputted image data (Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Fig. 1: plurality of image data processing means); and

an image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager), where

the image processing system distributes image data received from the image data processing requesting means to the second image data processing means available for distributed processing in addition to the first image data processing means that is first requested to process the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision

Art Unit: 2438

block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202), wherein

the data processing requesting means have a function [to verify security levels] of the second image data processing means to which the image data distributed processing is to be requested (Paragraph 0101: check the status of the appliance queue associated with the selected device; Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons) and

then request the second image data processing means to perform distributed processing of the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202); and

the second image data processing means have a function to perform distributed processing of the image data in conjunction with the first image data processing means first requested to process the image data (Paragraph 0089: Documents 228 input to the thick client 222 are opened within a native application 230, and sent to the thick client

Art Unit: 2438

222 in response to a print command of the native application 230. Since the thin client 224 is browser-based for selecting documents from a server, the documents 228 are uploaded to the thin client 228. Additionally, the thin client 224 suitably communicates with a remote DMM 232 of a second appliance 234).

Verma does not explicitly disclose but Lunt from the same or similar fields of endeavor teaches verifying security levels in image processing system (Col. 4 lines 30-38: Once the policy 113 determines the security requirements, the print management system 112 identifies the specific combination of protection techniques needed to meet these requirements. The print management system 112 then routes the print job to one of the trusted printers 131 135 that can apply the appropriate protections and sets the parameters in the selected printer to apply the appropriate protection techniques to the document 140).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels as taught by Lunt in the teachings of Verma for the advantage of printing a document requiring forgery protection using a number of trusted printers (Col. 1 lines 55-57).

Regarding Claim 6, Verma discloses an image processing system, comprising: a plurality of image data processing means including at least first and second image data processing means which have different security levels and which process inputted image data (Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152:

Art Unit: 2438

access to DMM objects is restricted to authorized users for security reasons; Fig. 1: plurality of image data processing means); and

image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager), where

the image processing system alternated processes image data inputted by the image data processing requesting means to the second image data processing means available for alternate processing in place of the first image data processing means that is first requested to process the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202), wherein

the image data processing requesting means have a function [to verify a security level] of the second image data processing means to which the image data alternate processing is to be requested (Paragraph 0101: check the status of the appliance queue associated with the selected device; Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons) and

then request the second image data processing means to perform alternate processing of the inputted image data if the first image data processing means that is first requested to process the image data can no longer continue processing subsequent part of the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202); and

the second image data processing means has a function to perform alternate processing of the subsequent part of the image data in place of the first image data processing means that is first requested to process the image data (Paragraph 0202: Additionally, a facility is provided to the user through which aged files (documents that were not accessed within a specified period of time) are automatically moved to an alternative location).

Verma does not explicitly disclose but Lunt from the same or similar fields of endeavor teaches verifying security levels in image processing system (Col. 4 lines 30-38: Once the policy 113 determines the security requirements, the print management system 112 identifies the specific combination of protection techniques needed to meet these requirements. The print management system 112 then routes the print job to one of the trusted printers 131 135 that can apply the appropriate protections and sets the

Art Unit: 2438

parameters in the selected printer to apply the appropriate protection techniques to the document 140).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels as taught by Lunt in the teachings of Verma so the parameters of the selected trusted printer are set by a print management system to print images, including the copy evidence and/or tracing information, appropriate to the required level of protection (Col. 2 lines 21-27).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2438

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R./

Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438